

UNITED STATES DISTRICT COURT

for the
WESTERN DISTRICT OF OKLAHOMA

In the Matter of the Search of a)
(Briefly describe the property to be searched)
or identify the person by name and address)
Samsung Galaxy S24 Ultra with IMEI)
357994255899992, Currently Located at the)
Stillwater Police Department,)
701 South Lewis Street,)
Stillwater, Oklahoma 74074)

Case No: M-25-136-SM

APPLICATION FOR SEARCH WARRANT

I, a federal law enforcement officer or attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following property (*identify the person or describe property to be searched and give its location*):

See Attachment A

Located in the Western District of Oklahoma, there is now concealed (*identify the person or describe the property to be seized*):

See Attachment B

The basis for the search under Fed. R. Crim.P.41(c) is(*check one or more*):

- ☒ evidence of the crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section

18 U.S.C. § 2252(a)(2) & (b)(1)
18 U.S.C. § 2252(a)(4)(B) & (b)(2)

Offense Description

Receipt and Distribution of Child Pornography
Possession of and Access with Intent to View
Child Pornography

The application is based on these facts:

See attached Affidavit of Special Agent Blair Newman, Federal Bureau of Investigation, which is incorporated by reference herein.

☒ Continued on the attached sheet(s).

☐ Delayed notice of [No. of Days] days (*give exact ending date if more than 30 days*) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet(s).



Applicant's signature

Blair Newman
Special Agent
Federal Bureau of Investigation

Sworn to before me and signed in my presence.

Date: March 4, 2025



Judge's signature

City and State: Oklahoma City, Oklahoma

SUZANNE MITCHELL, U.S. Magistrate Judge

Printed name and title

**Affidavit in Support of an Application
Under Rule 41 for a Warrant to Search and Seize**

I, Blair Newman, being first duly sworn under oath, depose and state:

Introduction and Agent Background

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant authorizing the examination of property—an electronic device—which is currently in law enforcement possession, and the extraction from that property of electronically stored information described in Attachment B.

2. I am a federal law enforcement officer as defined under Rule 41(a)(2)(C) and am authorized to request this search warrant because I am a government agent who is engaged in enforcing federal criminal laws and I am within the category of officers authorized by the Attorney General to request such a warrant. I am a Special Agent with the Federal Bureau of Investigation (“FBI”) and have been since May 2019. I am assigned to the Tulsa Resident Agency of the Oklahoma City Division. My primary duties as a Special Agent with the FBI include but are not limited to investigating crimes against children.

3. Specifically, I have extensive experience working cases involving child pornography and child exploitation in violation of 18 U.S.C. §§ 2251, 2252, and 2252A. All these cases have required the review of child pornography (as defined in 18 U.S.C. § 2256) in all forms of media including computer media. As such, I am familiar with the tactics utilized by individuals who collect, distribute, and or produce child pornographic material.

4. I am familiar with the facts and circumstances of this investigation. The facts set forth in this affidavit are based on my personal observations, knowledge obtained from other law enforcement officers, my review of documents related to this investigation, conversations with others who have personal knowledge of the events and circumstances described herein, and a

review of open-source information including information available on the Internet. Because this affidavit is submitted for the limited purpose of establishing probable cause in support of the application for a search warrant, it does not set forth each and every fact I or others have learned during the course of this investigation.

5. Based on my training, experience, and the facts set forth in this affidavit, there is probable cause to believe that evidence of violations of Title 18 U.S.C. §§ 2252(a)(2) and (b)(1) (Receipt and Distribution of Child Pornography) and 18 U.S.C. §§ 2252(a)(4)(B) and (b)(2) (Possession of and Access with Intent to View Child Pornography) will be located in the electronically stored information described in Attachment B and is recorded on Target Device 1 described in Attachment A.

Jurisdiction

6. “[A] warrant may be issued to search for and seize any property that constitutes evidence of a criminal offense in violation of the laws of the United States.” 18 U.S.C. § 3103a.

7. The requested search is related to the following violations of federal law:

- a. Title 18, United States Code, Sections 2252(a)(4)(B) and (b)(2) prohibit any person from knowingly possessing or accessing with the intent to view, or attempting or conspiring to possess or access with the intent to view, one or more books, magazines, periodicals, films, video tapes, or other matter which contain any visual depiction that has been mailed, or has been shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce, or which was produced using materials which have been mailed or so shipped or transported, by any means including by computer, if the production of such visual depiction involved the use of a minor engaging in sexually explicit conduct and such visual depiction is of such conduct.

8. Venue is proper because the person or property described in this affidavit is located within the Western District of Oklahoma. Fed. R. Crim. P. 41(b)(1).

Identification of the Device to be Examined

9. The property to be searched is a Samsung Galaxy S24 Ultra with IMEI 357994255899992 hereinafter “Target Device 1.” Target Device 1 is currently located at the Stillwater Police Department, 701 South Lewis Street, Stillwater, Oklahoma 74074, Western District of Oklahoma.

10. The applied-for warrant would authorize the forensic examination of Target Device 1 for the purpose of identifying electronically stored data particularly described in Attachment B.

Definitions

11. The following definitions, inclusive of all definitions contained in 18 U.S.C. § 2256, apply to this affidavit and the attachments incorporated herein:

- a. “Child pornography,” as defined in 18 U.S.C. § 2256(8), is any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical or other means, of sexually explicit conduct, where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct;
- b. “Internet Protocol address” or “IP address” refers to a unique number used by a computer or electronic device to access the Internet. IP addresses can be dynamic, meaning that the ISP assigns a different unique number to a computer every time it accesses the Internet. IP addresses may also be static, which means the ISP assigns

a user's computer a particular IP address that is used each time the computer accesses the Internet;

- c. "Electronic Mail," commonly referred to as email (or e-mail), is a method of exchanging digital messages from an author to one or more recipients. Modern email operates across the Internet or other computer networks. Email systems are based on a store-and-forward model; that is, email servers accept, forward, deliver, and store messages. Neither the users nor their computers are required to be online simultaneously; they need only connect briefly, typically to an email server, for as long a period of time as it takes to send or receive messages. One of the most common methods of obtaining an email account is through a free web-based email service provider such as, Outlook, Yahoo, or Gmail. Anyone with access to the Internet can generally obtain a free web-based email account;
- d. A "hash value" or "hash ID" is a unique alpha-numeric identifier for a digital file. A hash value is generated by a mathematical algorithm, based on the file's content. A hash value is a file's "digital fingerprint" or "digital DNA." Two files having identical content will have the same hash value, even if the file names are different. On the other hand, any change to the data in a file, however slight, will change the file's hash value, even if the file name is unchanged. Thus, if two files have the same hash value, they are said to be identical, even if they have different file names;
- e. "Cloud storage service" refers to a publicly accessible, online storage provider that can be used to store and share files in large volumes. Users of cloud storage services can share links and associated passwords to their stored files with others in order to grant access to their file collections. Such services allow individuals to easily access these files through a wide variety of electronic devices such as desktop computers,

laptops, mobile phones or tablets, from anywhere. Many services provide free access up to a certain size limit;

- f. The “Internet” is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state;
- g. “Minor,” as defined in 18 U.S.C. § 2256(1), refers to any person under the age of eighteen years;
- h. “Records,” “documents,” and “materials,” as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade, photographic, mechanical, electrical, electronic, or magnetic form;
- i. “Sexually explicit conduct,” as defined in 18 U.S.C. § 2256(2), means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any person; and
- j. “Visual depiction,” as defined in 18 U.S.C. § 2256(5), includes undeveloped film and videotape, data stored on computer disc or other electronic means which is capable of conversion into a visual image, and data which is capable of conversion into a visual image that has been transmitted by any means, whether or not stored in a permanent format.
- k. “Computer,” as defined in 18 U.S.C. § 1030(e)(1), means an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing

logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device.

Probable Cause

12. On August 7, 2024, FBI Agents interviewed Joseph Gunther Sampson, who confessed to viewing, receiving, and sending child pornography. Sampson provided Agents with consent to search multiple electronic devices, to include his iPhone SE. On September 16, 2024, Sampson was indicted in the Northern District of Oklahoma (24-CR-298) and charged with Receipt and Distribution of Child Pornography and Possession of Child Pornography in Indian Country.

13. In November 2024, I reviewed an extraction of Sampson's iPhone SE and identified text messages sent between Sampson and telephone number 405-564-2463, which law enforcement databases and open-source research identified as belonging to Cody Ryan Richison, date of birth XX/XX/1990, and home address 2963 N 375 Road, Holdenville, Oklahoma 74848. Research further revealed Richison was an Agricultural Education Instructor at Holdenville High School and a Future Farmers of America (FFA) Advisor. The text messages were exchanged on January 26, 2024, and included the following:

Sampson: You really want to do the pedo¹ family thing?

Richison: Yes I do. Do you?

Sampson: God yes

...

Sampson: You fucked an underage?

...

Sampson: Whats youngest youve been in?

...

Richison: 10

¹ I know from my training and experience that that the term "pedo" is a slang reference for "pedophilia."

Sampson: Hmmm fuck yes

Richison: A buddy's foster son.

Richison: There's a guy in henryetta that has a 3-4 yo

Sampson: 😊

Richison: He's on Tele

14. Richison was also the subject of National Center for Missing and Exploited Children (NCMEC) CyberTipline Report 197677580. According to the report, Witness 1 called to report his ex-partner, Witness 2, confessed to him in April 2024 that he was cheating on him with Richison. Witness 2 also disclosed to Witness 1 that Richison was in possession of child pornography on his cell phone. Witness 2 stated that one day Richison left his phone unlocked and he observed child pornography on it.

15. On December 4, 2024, the Oklahoma State Bureau of Investigation (OSBI) provided the FBI with a copy of text messages sent between Cody Allen Stolfa² and telephone number 405-564-2463, belonging to Richison. The text messages were exchanged between March 10, 2024, and March 12, 2024, and included the following:

Stolfa: Hahaha there is a boy here in town that I get to use

Richison: Damn How old?

Stolfa: 16

Richison: You are so fucking lucky! I can't stand you. Lol what's he look like?

Stolfa: Hmmm I know I've got a body/dick pic. One sec

Stolfa: [image000000.jpg]

Richison: Oh fuuuuuck

Stolfa: Lmao

Richison: I hate you lol

16. On January 27, 2025, I reviewed "image000000.jpg," sent from Stolfa to Richison on March 10, 2024. "image000000.jpg" was a mirror selfie of a nude post-pubescent male. The male

² Cody Allen Stolfa is an individual known to law enforcement and is currently the subject of a prosecution for child exploitation.

had dark brown hair, a light mustache, and acne on his right cheek. The male was holding an Android smartphone in a black case in his right hand. The male had dark brown pubic hair, and his penis was erect and exposed. According to the text messages, Stolfa said the male was 16 years old. However, Stillwater Police Department was not yet able to identify and/or locate the male.

17. On December 4, 2024, Agents executed three sealed, federal search warrants for the person of CODY RYAN RICHISON, a premises at 2963 N 375 Road, Holdenville, Oklahoma 74848, and the white Ford F-150 truck with VIN 1FTPW14V19FA70397, respectively 24-MJ-394-DES, 24-MJ-393-DES, and 24-MJ-392-DES. During the execution of the search warrants, Agents located Richison, who agreed to speak with Agents. During a post-Miranda interview, Richison made numerous incriminating statements, including but not limited to:

- Richison received approximately 100 photos and videos of children being sexually abused from Stolfa, beginning in approximately 2020. The children being sexually abused were both male and female, and their ages ranged, but included children as young as infants. Richison received at least one of these images in March 2024 while he was employed as a teacher at Holdenville High School in the Eastern District of Oklahoma. Richison knew his actions were wrong.
- Richison worked with children every day. Richison recently talked with a friend about becoming a foster parent.
- Richison knew what happened to “CHOMOS”³ in prison because he previously worked in a correctional facility.

18. Target Device 1 is currently in the lawful possession of the Stillwater Police Department. Target Device 1 came into Stillwater Police Department’s possession on July 10,

³ I know from my training and experience that the term “chomos” is a slang reference for “child molesters.”

2024, when the Stillwater Police Department arrested Stolfa at Boomer Creek Apartments, 320 East McElroy Road, Stillwater, Oklahoma 74075, and seized Target Device 1 pursuant to Stolfa's arrest.

19. On July 16, 2024, Stillwater Police Department obtained a search warrant signed by the Honorable Judge Worthington of Payne County, Oklahoma to search Target Device 1.

20. Pursuant to the search warrant, OSBI performed the extraction of Target Device 1 on August 15, 2024. On August 29, 2024, Detective Wheeler completed review of Target Device 1 and located, among other things:

- Images: 87 images of CSAM involving pubescent and prepubescent minors; 55 images involving "age difficult" pornographic material.
- Videos: 13 videos of CSAM involving pubescent and prepubescent minors; 18 videos involving "age difficult" pornographic material.

21. Target Device 1 is currently in Stillwater Police Department custody in the Stillwater Police Department Property Unit, located at 701 South Lewis Street, Stillwater, Oklahoma 74074, Western District of Oklahoma. In my training and experience, I know that Target Device 1 has been stored in a manner in which its contents are, to the extent material to this investigation, in substantially the same state as they were when Target Device 1 first came into the possession of Stillwater Police Department.

Technical Terms

22. Based on my training and experience, I use the following technical terms to convey the following meanings:

- a. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of

transmitter/receivers, enabling communication with other wireless telephones or traditional “land line” telephones. A wireless telephone usually contains a “call log,” which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include storing names and phone numbers in electronic “address books;” sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system (“GPS”) technology for determining the location of the device.

- b. Digital camera: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.
- c. Portable media player: A portable media player (or “MP3 Player” or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage media. Removable storage media include various types of flash memory cards or miniature hard drives.

This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.

- d. GPS: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated “GPS”) consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna’s latitude, longitude, and sometimes altitude with a high level of precision.
- e. PDA: A personal digital assistant, or PDA, is a handheld electronic device used for storing data (such as names, addresses, appointments or notes) and utilizing computer programs. Some PDAs also function as wireless communication devices and are used to access the Internet and send and receive e-mail. PDAs usually include a memory card or other removable storage media for storing data and a keyboard and/or touch screen for entering data. Removable storage media include various types of flash memory cards or miniature hard drives. This removable

storage media can store any digital data. Most PDAs run computer software, giving them many of the same capabilities as personal computers. For example, PDA users can work with word-processing documents, spreadsheets, and presentations. PDAs may also include global positioning system (“GPS”) technology for determining the location of the device.

- f. IP Address: An Internet Protocol address (or simply “IP address”) is a unique numeric address used by computers on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet computer must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.
- g. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

23. Based on my training, experience, and research, I know that Target Device 1 has capabilities that allow it to serve as a wireless telephone, digital camera, portable media player, GPS navigation device, and PDA. In my training and experience, examining data stored on devices of these types can uncover, among other things, evidence that reveals or suggests who possessed or used Target Device 1.

**Characteristics Common to Individuals
who Exhibit a Sexual Interest in Children and Individuals who Distribute, Receive, Possess
and/or Access with Intent to View Child Pornography**

24. Based on my previous investigative experience related to child exploitation investigations, and the training and experience of other law enforcement officers with whom I have had discussions, I know there are certain characteristics common to individuals who distribute, receive, possess, and/or access with intent to view child pornography:

- a. Such individuals may receive sexual gratification, stimulation, and satisfaction from contact with children, or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media, or from literature describing such activity;
- b. Such individuals may collect sexually explicit or suggestive materials in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or drawings or other visual media. Individuals who have a sexual interest in children or images of children oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts;
- c. Such individuals almost always possess and maintain digital or electronic files of child pornographic material, that is, their pictures, videos, photographs, correspondence, mailing lists, etc., in the privacy and security of their home or some other secure location. Individuals who have a sexual interest in children or images of children typically retain pictures, videos, photographs, correspondence, and mailing lists for many years;

- d. Likewise, such individuals often maintain their child pornography images in a digital or electronic format in a safe, secure and private environment, such as a computer and surrounding area. These child pornography images are often maintained for several years and are kept close by, usually at the possessor's residence, inside the possessor's vehicle, or, at times, on their person, to enable the individual to view the child pornography images, which are valued highly. Some of these individuals also have been found to download, view, and then delete child pornography on their computers or digital devices on a cyclical and repetitive basis;
- e. Based on my training and experience and speaking with other special agents, I know that such individuals have taken their electronic devices and storage media, which contain their collections of child pornography, with them when they have moved or changed residences;
- f. Such individuals may also take it upon themselves to create their own child pornography or child erotica images, videos or other recordings, or engage in contact sex offenses with children. These images, videos or other recordings may be taken or recorded covertly, such as with a hidden camera in a bathroom, or the individual may have child victims he or she is abusing in order to produce child pornographic or child erotica images, videos or other recordings. Studies have shown there is a high cooccurrence between those who traffic in child pornography and commit sex offenses with children. Such individuals may also attempt to persuade, induce, entice, or coerce child victims in person or via communication devices to self-produce and send them child pornography or to

meet in person for sex acts. These images, videos or other recordings are often collected, traded, or shared;

- g. Importantly, evidence of such activity, including deleted child pornography, often can be located on these individuals' computers and digital devices through the use of forensic tools. Indeed, the very nature of electronic storage means that evidence of the crime is often still discoverable for extended periods of time even after the individual "deleted"⁴ it;
- h. Such individuals also may correspond with and/or meet others to share information and materials, rarely destroy correspondence from other child pornography distributors/possessors, conceal such correspondence as they do their sexually explicit material, and often maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography;
- i. Based on my training and experience, I know that such individuals may use their financial information to buy and sell child pornography online and purchase software used to mask their online activity from law enforcement. For instance, individuals may purchase cryptocurrency such as Bitcoin to buy and sell child pornography online. The use of cryptocurrency provides a level of anonymity because it masks the user's identity when conducting online financial transactions and provides a means of laundering illicit proceeds. Financial information may provide a window into the identities of individuals seeking to buy or sell child

⁴ See *United States v. Carroll*, 750 F.3d 700, 706 (7th Cir. 2014) (concluding that 5-year delay was not too long because "staleness inquiry must be grounded in an understanding of both the behavior of child pornography collectors and of modern technology"); see also *United States v. Seiver*, 692 F.3d 774 (7th Cir. 2012) (Posner, J.) (collecting cases, e.g., *United States v. Allen*, 625 F.3d 830, 843 (5th Cir. 2010); *United States v. Richardson*, 607 F.3d 357, 370–71 (4th Cir. 2010); *United States v. Lewis*, 605 F.3d 395, 402 (6th Cir. 2010).)

pornography online by tying the illicit transactions back to the user. Financial information contained on an electronic device containing child pornography may also provide indicia of ownership. Further, based on my training and experience, I know that individuals involved in the trafficking of child pornography may use sophisticated software, such as router configuration software, virtual private networks, proxy servers, cryptocurrency exchanges, or other anonymizing software, in conjunction with these illicit financial transactions to provide dual layers of anonymity and prevent law enforcement detection. Financial information may indicate which services were purchased to obscure an individual's identity;

- j. Such individuals prefer not to be without their child pornography for any prolonged period of time. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world.

Background on Child Pornography, Computers, and the Internet

25. I have had both training and experience in the investigation of computer-related crimes.

Based on my training, experience, and knowledge, I know the following:

- a. Computers, smartphones and digital technology are the primary way in which individuals interested in child pornography interact with each other. Computers and smartphones basically serve four functions in connection with child pornography: production, communication, distribution, and storage;
- b. Digital cameras and smartphones with cameras save photographs or videos as a digital file that can be directly transferred to a computer by connecting the camera or smartphone to the computer, using a cable or via wireless connections such as

“Wi-Fi” or “Bluetooth.” Photos and videos taken on a digital camera or smartphone may be stored on a removable memory card in the camera or smartphone. These memory cards are often large enough to store thousands of high-resolution photographs or videos;

- c. A device known as a modem allows any computer to connect to another computer through the use of telephone, cable, or wireless connection. Mobile devices such as smartphones and tablet computers may also connect to other computers via wireless connections. Electronic contact can be made to literally millions of computers and smartphones and tablets around the world. Child pornography can therefore be easily, inexpensively and anonymously (through electronic communications) produced, distributed, and received by anyone with access to a computer or smartphone;
- d. The computer’s ability to store images in digital form makes the computer itself an ideal repository for child pornography. Electronic storage media of various types – to include computer hard drives, external hard drives, CDs, DVDs, and “thumb,” “jump,” or “flash” drives, which are very small devices which are plugged into a port on the computer – can store thousands of images or videos at very high resolution. It is extremely easy for an individual to take a photo or a video with a digital camera or camera-bearing smartphone, upload that photo or video to a computer, and then copy it (or any other files on the computer) to any one of those media storage devices. Some media storage devices can easily be concealed and carried on an individual’s person. Smartphones and/or mobile phones are also almost always carried on an individual’s person (or within their immediate dominion and control) and can additionally store media;

e. The Internet affords individuals several different venues for obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion;

f. Individuals also use online resources to retrieve and store child pornography.

Some online services allow a user to set up an account with a remote computing service that may provide e-mail services and/or electronic storage of computer files in any variety of formats. A user can set up an online storage account (sometimes referred to as “cloud” storage) from any computer or smartphone with access to the Internet. Even in cases where online storage is used, however, evidence of child pornography can be found on the user’s computer, smartphone or external media in most cases; and

g. As is the case with most digital technology, communications by way of computer or smartphone can be saved or stored on the computer or smartphone used for these purposes. Storing this information can be intentional (i.e., by saving an e-mail as a file on the computer or smartphone, or saving the location of one’s favorite websites in, for example, “bookmarked” files). Digital information can also be retained unintentionally such as the traces of the path of an electronic communication may be automatically stored in many places (e.g., temporary files or ISP client software, among others). In addition to electronic communications, a computer or smartphone user’s Internet activities generally leave traces or “footprints” in the web cache and history files of the browser used. Such information is often maintained indefinitely until overwritten by other data.

Electronic Storage and Forensic Analysis

26. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

27. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how Target Device 1 was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on Target Device 1 because:

- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).
- b. Forensic evidence on a device can also indicate who has used or controlled the device. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence.
- c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.
- d. The process of identifying the exact electronically stored information on a storage medium that is necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is

evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

- e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

28. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the device consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

29. *Manner of execution.* Because this warrant seeks only permission to examine a device already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

30. *Methods of examination.* In conducting this examination, law enforcement personnel may use various methods to locate evidence and instrumentalities of the crime(s) under investigation, including but not limited to undertaking a cursory inspection of all information within Target Device 1. This method is analogous to cursorily inspecting all the files in a file cabinet in an office to determine which paper evidence is subject to seizure. Although law enforcement personnel may use other methods as well, particularly including keyword searches, I know that keyword searches and similar methods are typically inadequate to detect all information subject to seizure. As an initial matter, keyword searches work only for text data, yet many types

of files commonly associated with stored cellular device data, such as pictures and videos, do not store as searchable text. Moreover, even as to text data, keyword searches cannot be relied upon to capture all relevant communications associated with a cellular device, as it is impossible to know in advance all of the unique words or phrases investigative subjects will use in their communications. Consequently, often many communications in cellular device data that are relevant to an investigation do not contain any searched keywords.

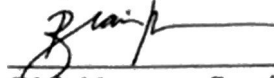
Conclusion

31. Based on the information set forth in this affidavit, I submit there is probable cause to believe that 18 U.S.C. §§ 2252(a)(2) and (b)(1) (Receipt and Distribution of Child Pornography) and 18 U.S.C. §§ 2252(a)(4)(B) and (b)(2) (Possession of and Access with Intent to View Child Pornography) have been violated, and that evidence of these offenses, more fully described in Attachment B, are located on Target Device 1 as described in Attachment A. I respectfully request that this Court issue a search warrant for the property described in Attachment A, authorizing the seizure of the items described in Attachment B.

32. I am aware that the recovery of data by a computer forensic analyst takes significant time; much the way recovery of narcotics must later be forensically evaluated in a lab, digital evidence will also undergo a similar process.

33. I request to be allowed to share this affidavit and the information obtained from this search with any government agency, to include state and local agencies investigating or aiding in the investigation of this case or related matters, and to disclose those materials as necessary to comply with discovery and disclosure obligations in any prosecutions from this matter.

Respectfully submitted,



Blair Newman, Special Agent
Federal Bureau of Investigation

Subscribed and sworn before me on March 4, 2025.



SUZANNE MITHCELL
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

Property to be Searched

The property to be searched is a Samsung Galaxy S24 Ultra with IMEI 357994255899992 hereinafter the Target Device 1. Target Device 1 is currently located at the Stillwater Police Department, 701 South Lewis Street, Stillwater, Oklahoma 74074, Western District of Oklahoma.

This warrant authorizes the forensic examination of Target Device 1 for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

Particular Things to be Seized

All records on Target Device 1 described in Attachment A that relate to violations of Title 18 U.S.C. §§ 2252(a)(2) and (b)(1) (Receipt and Distribution of Child Pornography) and 18 U.S.C. §§ 2252(a)(4)(B) and (b)(2) (Possession of and Access with Intent to View Child Pornography), specifically:

- A. All communications or other messages Cody Stolfa sent to or received from Cody Richison, with phone number 405-564-2463, including iMessages, SMS messages, and all other forms of text message;
- B. Images/videos/gifs of child pornography or child erotica; files containing images/videos/gifs; and data of any type relating to the sexual exploitation of minors or a sexual interest in children, material related to the possession thereof, and data of any type related to any person employing, using, persuading, inducing, enticing, or coercing any minor to engage in any sexually explicit conduct for the purpose of producing any visual depiction of such conduct or for the purpose of transmitting such visual depiction of such conduct, in any form wherever it may be stored or found, materials shared with or between Cody Stolfa and Cody Richison including, but not limited to:
 - i. Graphic Interchange formats and/or photographs, and other visual depictions of such Graphic Interchange formats (including, but not limited to, JPG, GIF, TIF, AVI, and MPEG) of child pornography; files relating to the distribution, receipt, or possession of child pornography, or information pertaining to an interest in child pornography;

- ii. Files in any form containing the visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256 or relating to the sexual exploitation of minors; and
- iii. Stories, text-based files, motion pictures, films, videos, and other recordings of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256 or relating to the sexual exploitation of minors.

C. Information, correspondence, records, documents or other materials shared with or between Cody Stolfi and Cody Richison pertaining to the possession, receipt or distribution of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256, or pertaining to the sexual exploitation of minors or a sexual interest in children, that were transmitted or received using computer, cellular device, personal digital assistant, or some other facility or means of interstate or foreign commerce, common carrier, or the U.S. mail including, but not limited to:

- i. Correspondence including, but not limited to, electronic mail, chat logs, and electronic messages, establishing possession, access to, or transmission through interstate or foreign commerce, including by United States mail or by computer, of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256 or relating to the sexual exploitation of minors or a sexual interest in children shared with or between Cody Stolfi and Cody Richison;
- ii. Any and all electronic and/or digital records and/or documents shared with or between Cody Stolfi and Cody Richison, pertaining to the preparation,

purchase, and acquisition of names or lists of names to be used in connection with the purchase, sale, trade, or transmission, through interstate commerce including by United States mail or by computer, any visual depiction of a minor engaged in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256 or relating to the sexual exploitation of minors;

- iii. Any and all electronic and/or digital records and/or documents shared with or between Cody Stolfi and Cody Richison, including any and all address books, names, and lists of names and addresses of minors visually depicted while engaging in sexually explicit conduct, defined in Title 18, United States Code, Section 2256; or relating to the sexual exploitation of minors;
- iv. Any and all records of Internet usage including usernames and e-mail addresses and identities assumed for the purposes of communication on the Internet. These records may include billing and subscriber records, chat room logs, e-mail messages, and include electronic files in a computer and on other data storage mediums;
- v. Any physical keys, encryption devices, dongles and similar physical items necessary to access computer equipment, storage devices or data;
- vi. Any passwords, password files, test keys, encryption codes or other information necessary to access the computer equipment, storage devices or data; and

vii. Files, records, programs, logs, electronic communications, scanning programs, financial records, hacking software, or router configuration software.

D. Records or other items which evidence ownership, use, or control of Target Device 1 described in Attachment A.

E. Credit card information including but not limited to bills and payment records, including but not limited to records of internet access.

F. Any and all information, correspondence (including emails), records, documents and/or other materials related to contacts, in whatever form, shared with or between Cody Stolfi and Cody Richison, with minors involving the production, possession and/or distribution of child pornography and the attempt or act of educating, enticing, coercing, or persuading a minor to engage in sexual acts.

As used above, the terms “records” and “information” includes all forms of creation or storage, including any form of computer or electronic storage.

The term “computer” includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term “storage medium” includes any physical object upon which computer data can be recorded, including external and internal hard drives, flash drives, thumb drives, micro-SD cards, macro-SD cards, DVDs, gaming systems, SIM cards, cellular phones capable of storage, floppy disks, compact discs, magnetic tapes, memory cards, memory chips, and other magnetic or optical media.

This warrant authorizes a review of electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to locate evidence, instrumentalities, contraband, and/or fruits described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.